Securing Location-Aware Services Based on Online/Offline Signatures in VANETs

Chul Sur, Youngho Park, Takashi Nishide, Kouichi Sakurai, Kyung Hyune Rhee

Securing Location-Aware Services Based on Online/Offline Signatures in VANETs*

Chul Sur[1], Youngho Park[2], Takashi Nishide[1],
Kouichi Sakurai[1], and Kyung Hyune Rhee[2]**

[1] Graduate School of Information Science and Electrical Engineering,
Kyushu University, Japan
{chulsur,nishide,sakurai}@itslab.csce.kyushu-u.ac.jp
[2] Department of IT Convergence and Application Engineering,
Pukyong National University, Republic of Korea
{pyhoya,khrhee}@pknu.ac.kr

Abstract. In this paper, we propose a novel privacy-preserving location assurance protocol for secure location-aware services over vehicular ad hoc networks (VANETs). In particular, we introduce the notion of location-aware credentials based on "hash-sign-switch" paradigm so as to guarantee the trustworthiness of location in location-aware services while providing conditional privacy preservation which is a desirable property for secure vehicular communications. Furthermore, the proposed protocol provides efficient procedures that alleviate a burden of computation for location-aware signature generation and verification on vehicles in VANETs. In order to achieve these goals, we consider online/offline signature scheme and identity-based aggregate signature scheme as our building blocks. Finally, we demonstrate experimental results to confirm the efficiency and effectiveness of the proposed protocol.

Keywords : VANETs, Location Assurance, Privacy Preservation, Location-Aware Credential, Online/Offline Signatures

1 Introduction

Vehicular ad hoc networks (VANETs) have emerged as a promising research field to provide significant opportunities for the deployment of a variety of applications and services as well as intelligent transportation systems to users. A VANET mainly consists of on-board units (OBUs) and roadside units (RSUs), where OBUs are installed on vehicles to provide wireless communication capability, while RSUs are deployed to provide access point to vehicles within their radio coverage. By this organization, the VANET enables useful functions, such

* This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government(Ministry of Education, Science and Technology).[NRF-2010-357-D00223]

** Corresponding author

as cooperative driving and probe vehicle data, that increase vehicular safety and reduce traffic congestion, and offer access to location-aware service applications.

A location-aware service on a VANET is to provide time-sensitive and higher-level services that distribute on-demand information such as traffic conditions, weather, and available facilities (e.g., gas station or restaurant) for a certain geographic area of interest by taking advantage of vehicular communications [4]. For the sake of supporting such a useful service, Dikaiakos et al. [4] proposed the development and deployment of location-aware service infrastructure on top of emerging VANETs based on a vehicular information transfer protocol (VITP) [5] which is an application layer communication protocol specifying the syntax and the semantics of messages for a VANET service. However, VITP does not provide built-in security features although it is necessary to develop a suit of elaborate and carefully designed security mechanisms before all other implementation aspects of VANETs [17].

Upon taking security design for viable location-aware service applications into consideration, location assurance is a fundamental security requirement from user's perspective because location information is an indispensable aspect for guaranteeing a reliable and trustworthy location-aware service. Recent advances in localization technologies enable accurate location estimation of vehicles based on transmission signal properties such as signal strength and direction. Prior location verification schemes [11, 16, 18] in the literature focused on secure packet forwarding in geographic routing protocol to identify a false node, which fakes its position, by verifying whether a neighbor node physically resides within a communication range. However, this approach is different from our protocol, and further, cannot support location assurance from the view of location-aware service.

On the other hand, sensitive information such as the identity and location privacy of a vehicle should be preserved from being illegally traced by a global eavesdropping attacker through vehicular communications [17]. To satisfy the requirement of privacy preservation, a variety of privacy-preserving authentication protocols have been proposed on the basis of digital signature including group signature schemes and anonymous certificates using pseudonyms of vehicles to conceal the real identities of vehicles [12, 13, 15]. However, those protocols cannot fulfill the location assurance requirement in our mind. Moreover, the requirement of location assurance seems to conflict with location privacy.

Our Contribution. In this paper, we propose a novel and efficient privacy-preserving location assurance protocol that addresses the conflicting goals of privacy preservation and location assurance for location-aware services over VANETs. Even though ordinary digital signature schemes are sufficient to guarantee the authenticity of a message including location information, it is insufficient to guarantee the semantics that the message was responded from a vehicle that passed through the claimed location since there is no binding between the signature function and the location information. Consequently, we introduce the notion of location-aware credential which is a signature on a trapdoor hash

value [10] under geographic location information and can be transformed into location-aware signatures on location-aware messages by applying "hash-sign-switch" paradigm [20] without violating location privacy of vehicles through vehicular communications. Moreover, the proposed protocol gains merit from the performance point of view by providing efficient signature generation and even verification on vehicles. In order to achieve these goals, we elaborately incorporate online/offline signatures [3] with an identity-based aggregate signature scheme [19] to generate location-aware credentials and signatures for location assurance, and make use of pseudonym-based anonymous authentication for privacy preservation.

2 System Model

2.1 Architecture

In this section, we describe our system model, in which communication nodes are either the trusted authority (TA), RSUs, or OBUs. The detailed description of system components is as follows:

- **TA** is public agencies or corporations with administrative powers in a specific field; for example, city or state transportation authorities. The TA is in charge of the registration of RSUs and vehicles deployed on a VANET, and issues cryptographic quantities through initial registration. In addition, the TA should be able to trace the real identity of a message originator by law enforcement when a problematic situation occurs.
- **RSUs** are subordinated to the TA and responsible for issuing location-aware credentials to each vehicle within RSUs' geographic areas. They assist the TA to resolve dispute cases and may not disclose any inner information without the authorization of the TA.
- **OBUs** are installed on the vehicles. They communicate with other OBUs for sharing location-aware information, and with RSUs for requesting the location-aware credentials used to generate signatures for a secure location-aware service.

To define architectural model more clearly, we make the following assumptions:

- RSUs are able to establish a secure channel with the TA by the Internet or any other reliable communication links with high bandwidth.
- Vehicles are equipped with an embedded computer, a GPS receiver, a wireless network interface compliant to standards like 802.11p incorporated with dedicated short range communications (DSRC) [21].
- A number of roadside service facilities (e.g., gas stations, coffee shops, restaurants, etc) are also equipped with short-range wireless interfaces and participate in the VANET.
- The TA can inspect all RSUs at high level and maintain the compromised entities list.

Since the main goal of this paper is to design security protocol, we do not describe the process of location-aware service transactions in detail. Instead, we assume the functionalities of the VITP [5] for our underlying location-aware service on VANETs. Multi-hop message delivery can be supported by geographic routing protocol such as GPSR [8], which forwards messages toward their geographic destination.

2.2 Security Objectives

Here we clarify our security objectives in order to provide secure and trustworthy location-aware services among vehicles in VANET environments. The concerns of our design are summarized as follows:

- **Location Assurance.** A location-aware service should guarantee the semantics that the information about a certain location of interest is related to the claimed target location. That is, it must be possible for a requesting vehicle to verify that a response message was actually originated from a vehicle within the target location area.
- **Authentication.** Only legitimate entities should take part in the VANETs. In addition, the origin of the messages should be authenticated to guard against the impersonation and message forgery attacks.
- **Location Tracking Avoidance.** The real identity and location privacy of a vehicle should be preserved from illegal tracing through a vehicular communication even though location assurance is supported.
- **Traceability.** The authority should be able to trace the originator of a message by revealing the real identity in case of any disputed situation such as liability investigation. That is, privacy preservation protocols in a VANET must be conditional by way of precaution against problematic situations.

3 Proposed Protocol

In this section, we present an efficient privacy-preserving location assurance protocol consisting of system setup, OBU and RSU registration, location-aware credential issuance, and location-aware signature generation and verification. To design the protocol, we consider identity-based authenticated key agreement scheme [2] for mutual authentication between an OBU and an RSU, and online/offline signatures [3] and identity-based aggregate signature scheme [19] for efficient location-aware signature generation and verification, respectively. Especially, the essence of our protocol is to use location-aware credentials based on "hash-sign-switch" paradigm [20] for providing reliable and trustworthy location-aware services without violating the location privacy of OBUs. Table 1 describes the notations used in the proposed protocol.

Table 1. Notations

Notation	Description
$params$	public system parameters
sk_i, vk_i	signing/verification key pair of entity i
ok_i, rk_j	identity-based secret keys for OBU_i and RSU_j, respectively
HK_i, TK_i	hash key and trapdoor key for OBU_i, respectively
$\Sigma_{i,j}$	location-aware credential for OBU_i issued from RSU_j
H_1, H_2, H_3, H_4, H_5	cryptographic hash functions
$\mathcal{L}_j$	location information of RSU_j
T	valid time period
MAC_k	MAC function under the key k
Enc_k, Dec_k	symmetric encryption and decryption functions under the key k, respectively
KDF	key derivation function

3.1 System Setup

The TA generates the required groups and public system parameters according to [2, 3, 19]. The TA chooses a multiplicative group $\mathbb{G}$ of the prime order p and bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2)$ of the same prime order q, then random generators $g \in \mathbb{G}$, $P \in \mathbb{G}_1$. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a bilinear map. The TA picks random $\gamma \in \mathbb{Z}_p^*$, $\alpha \in \mathbb{Z}_q^*$ as the master keys for identity-based cryptography and sets $g_0 = g^\gamma$, $P_0 = \alpha P$ as the corresponding public keys, respectively. The TA also chooses cryptographic hash functions which are defined as $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$ and $H_3, H_4, H_5 : \{0,1\}^* \to \mathbb{Z}_p^*$.

In addition, the TA chooses a collision resistant one-way hash function h and a secure symmetric encryption algorithm Enc, then defines a key derivation function KDF built on the hash function h. Finally, it publishes the public system parameter $params = \{\mathbb{G}, \mathbb{G}_1, \mathbb{G}_2, g, g_0, e, P, P_0, H_1, H_2, H_3, H_4, H_5, Enc, KDF\}$.

3.2 OBU and RSU Registration

In our system, all OBUs and RSUs need to be registered from the TA and preloaded with their own secret quantities before joining a VANET. Fig. 1 describes the procedure of initial registration with respect to OBUs and RSUs, respectively.

If the registration entity is an OBU_i, it submits its own real identity ID_i to the TA. Then the TA first checks its validity. If the identity ID_i passes the check, it derives a pseudo identity $\mathsf{PID}_i = Enc_K(\mathsf{ID}_i)$ under the secret key K from OBU_i's real identity ID_i, then computes $ok_i = \alpha H_1(\mathsf{PID}_i)$ as OBU_i's identity-based secret key used for mutual authentication with RSUs. The TA transmits $\langle params, \mathsf{PID}_i, ok_i \rangle$ to OBU_i and registers $\langle \mathsf{ID}_i, \mathsf{PID}_i \rangle$ as a legitimate entity in secure storage.

Registration for $\mathtt{OBU}_i$

1. Generate $\mathsf{PID}_i = Enc_K(\mathsf{ID}_i)$ as OBU_i's pseudo identity.
2. Compute $ok_i = \alpha H_1(\mathsf{PID}_i)$ as OBU_i's identity-based secret key.
3. Issue $\langle params, \mathsf{PID}_i, ok_i \rangle$ to OBU_i.

Registration for $\mathtt{RSU}_j$

1. Compute $rk_j = \alpha H_1(\mathcal{L}_j||T)$ as RSU_j's identity-based secret key.
2. Choose $s_j \in \mathbb{Z}_p^*$ and compute $\Delta_j = g^{s_j}$.
3. Set $sk_j = s_j + \gamma H_3(\mathcal{L}_j||T||\Delta_j) \pmod p$ as RSU_j's signing key.
4. Issue $\langle params, rk_j, sk_j, \Delta_j \rangle$ to RSU_j.

Fig. 1. Initial registration for OBUs and RSUs by the TA

On the other hand, if the registration entity is an RSU_j, the TA computes $rk_j = \alpha H_1(\mathcal{L}_j||T)$ and $sk_j = s_j + \gamma H_3(\mathcal{L}_j||T||\Delta_j) \pmod p$ using the location information $\mathcal{L}_j$ in which RSU_j is located together with the valid time period T. At this step, rk_j is an identity-based secret key used for mutual authentication with OBUs and sk_j is a signing key which is used for issuing location-aware credentials for assuring location-aware services in VANETs, respectively. Then the TA issues $\langle params, rk_j, sk_j, \Delta_j \rangle$ to the RSU_j.

Remark 1. According to [4], a location information $\mathcal{L}$ can be represented as two-value tuples [road-ID, segment-ID], where road-ID is a unique key representing a road and segment-ID is a number representing a segment of that road [14]. Given that the movement of vehicles is constrained within the road system, we can assume that the geographic areas of interest are restricted to roads and road segments. Therefore, those representations can be used as identifiers for our key generation.

Remark 2. The valid time period T used in our protocol makes fine-grained revocation possible with respect to RSU_j's identity-based secret quantities. For instance, if the TA sets the valid time period T as current date to generate $rk_j = \alpha H_1(\mathcal{L}_j||T)$ and $sk_j = s_j + \gamma H_3(\mathcal{L}_j||T||\Delta_j)$, the vulnerability window of RSU_j is restricted to the end of the day since RSU_j's secret keys are inherently useless after current date. Moreover, the process of secret key renewal on the TA is insignificant operation since only hash function, 1 point multiplication of $\mathbb{G}_1$ and 1 modular exponentiation of $\mathbb{Z}_p^*$ are used in our protocol and pre-computations are also possible.

3.3 Location-Aware Credential Issuance

When an OBU_i wants to get a new location-aware credential for joining secure location-aware service from the RSU_j located in the OBU_i's geographic area, the OBU_i and the RSU_j perform a location-aware credential issuance protocol.

The proposed protocol is composed of two phases. One is mutual authentication between the OBU_i and the RSU_j using their identity-based secret keys, and the other is a location-aware credential generation by the RSU_j. The detailed steps are as follows.

Step 1. The OBU_i picks a random $a \in \mathbb{Z}_q^*$ to compute $X = aP$ and generates $Q_i = H_1(\mathsf{PID}_i)$, then sends $\langle X, Q_i \rangle$ to the RSU_j as a request.

Step 2. Upon receiving the request, the RSU_j picks a random $b \in \mathbb{Z}_q^*$ and computes $Y = bP$. The RSU_j establishes $k = e(bQ_i, P_0) \cdot e(rk_j, X)$ and computes $\pi_j = MAC_{k_0}(Q_i, X, Y, \mathcal{L}_j, T)$, where $k_0 = KDF(k||0)$. Then the RSU_j sends $\langle Y, \mathcal{L}_j, T, \pi_j \rangle$ to the OBU_i as a response.

Step 3. The OBU_i also establishes $k = e(ok_i, Y) \cdot e(aQ_j, P_0)$ and checks that $\pi_j \stackrel{?}{=} MAC_{k_0}(Q_i, X, Y, \mathcal{L}_j, T)$ to authenticate the RSU_j, where $Q_j = H_1(\mathcal{L}_j||T)$ and $k_0 = KDF(k||0)$. If it holds, the OBU_i chooses a random $x_i \in \mathbb{Z}_q^*$ as a trapdoor key TK_i and sets $HK_i = x_i P$ as the corresponding hash key, respectively. Finally, the OBU_i computes $C_i = Enc_{k_1}(\mathsf{PID}_i, HK_i)$, where $k_1 = KDF(k||1)$ and $\pi_i = MAC_{k_0}(\mathsf{PID}_i, Q_i, X, Y, HK_i, \mathcal{L}_j, T)$, then transmits $\langle C_i, \pi_i \rangle$ to the RSU_j.

Step 4. First, the RSU_j decrypts C_i under $k_1 = KDF(k||1)$ to obtain OBU's pseudo identity PID_i and hash key HK_i. Then it looks up the up-to-date revocation list retrieved from the TA to check the validity of the given PID_i. If the PID_i is revoked one, the RSU_j refuses to issue a location-aware credential. Otherwise, it checks that $\pi_i \stackrel{?}{=} MAC_{k_0}(\mathsf{PID}_i, Q_i, X, Y, HK_i, \mathcal{L}_j, T)$. If the check holds, the RSU_j chooses a random $\lambda_i \in \mathbb{Z}_q^*$ and computes the trapdoor hash value $\xi_i = \lambda_i HK_i$. The RSU_j also picks a random $r \in \mathbb{Z}_p^*$, then generates a location-aware credential $\Sigma_{i,j} = (\Delta_j, U_i, V_i)$:

$$\begin{cases} U_i = g^r \\ V_i = r\psi_{i,0} + sk_j\psi_{i,1} \pmod{p} \end{cases}$$

where $\psi_{i,0} = H_4(\xi_i||\mathcal{L}_j||T||U_i||\Delta_j)$ and $\psi_{i,1} = H_5(\xi_i||\mathcal{L}_j||T||\psi_{i,0}||U_i||\Delta_j)$. Finally, the RSU_j computes $C_j = Enc_{k_1}(\lambda_i)$ and $\pi'_j = MAC_{k_0}(\lambda_i, \Sigma_{i,j})$, then transmits $\langle C_j, \Sigma_{i,j}, \pi'_j \rangle$ to the OBU_i. In addition, RSU_j stores $\langle \mathsf{PID}_i, HK_i \rangle$ in its local credential list for assisting the TA by way of provision against a liability investigation. Note that, in location-aware credential generation, no identity-related information is included in $\Sigma_{i,j}$.

Step 5. The OBU_i retrieves the secret value $\lambda_i = Dec_{k_1}(C_j)$, then checks $\pi'_j \stackrel{?}{=} MAC_{k_0}(\lambda_i, \Sigma_{i,j})$. If the check is valid, the OBU_i sets $sk_i = \langle TK_i, \lambda_i \rangle$ as its singing key and $vk_i = HK_i$ as its verification key, respectively.

Remark 3. The location-aware credential $\Sigma_{i,j} = (\Delta_j, U_i, V_i)$ for OBU_i is an identity-based signature on the trapdoor hash value ξ_i under the geographic location $\mathcal{L}_j$ and the valid time period T. Moreover, the location-aware credential $\Sigma_{i,j}$ can be re-used whenever OBU_i wants to sign a location-aware message during the specific time period T.

3.4 Location-Aware Signature Generation and Verification

Fig. 2 depicts the message structure used for a secure location-aware service. The type field represents either request or response. The target and source fields contain location area of interest that specifies the road and segment identifiers, as retrieved by an on-board navigation and positioning system. Hash_key and signature fields contain message originator's hash key and a digital signature on the message under location information and valid time period, respectively.

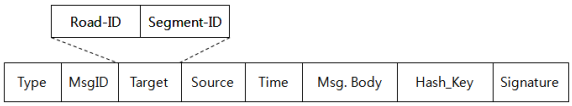


Fig. 2. Message structure

As aforementioned, since we assume an underlying VANET routing protocol, we just present how location-aware credential lead to location-aware signature generation and verification on the message for a secure and trustworthy location-aware service as shown in Fig. 3. For a given location-aware service message m, any entity in a VANET is able to convert a location-aware credential Σ into a location-aware signature σ on the message m by using its own trapdoor key TK during the valid time period T.

`Signature Generation` for given location-aware service message m and credential $\Sigma_{i,j}$, an OBU_i performs as follows:

1. Choose a random $c \in \mathbb{Z}_q^*$ and compute $\kappa = cP$.
2. Compute $\omega = \lambda_i - \delta c x_i^{-1} \pmod{q}$, where $\delta = H_2(m||\kappa)$.
3. Set $\sigma = (\kappa, \omega, \Sigma_{i,j})$ as a signature on m.

`Aggregate Verification` for n pairs (m_i, σ_i) where $i \in [1, n]$, the receiver performs as follows:

1. Compute $\delta_i = H_2(m_i||\kappa_i)$ and $\xi_i = \delta_i \kappa_i + \omega_i HK_i$ for $i \in [1, n]$.
2. Compute $\psi_{i,0} = H_4(\xi_i||\mathcal{L}_j||T||U_i||\Delta_j)$ and $\psi_{i,1} = H_5(\xi_i||\mathcal{L}_j||T||\psi_{i,0}||U_i||\Delta_j)$ for $i \in [1, n]$.
3. Check that $g^{\sum_{i=1}^{n} V_i} \stackrel{?}{=} \prod_{i=1}^{n} U_i^{\psi_{i,0}} \cdot \prod_{i=1}^{n} \Delta_j^{\psi_{i,1}} \cdot g_0^{\sum_{i=1}^{n} \psi_{i,1} H_3(\mathcal{L}_j||T||\Delta_j)}$.

Fig. 3. Location-aware signature generation and verification

The consistency of the location-aware signature verification can be proved as follows:

– For the trapdoor hash value ξ_i, we have that

$$\begin{aligned}\xi_i &= \delta_i\kappa_i + \omega_i HK_i \\ &= H_2(m_i||\kappa_i)\kappa_i + \omega_i HK_i \\ &= H_2(m_i||c_iP)c_iP + (\lambda_i - H_2(m_i||c_iP)c_ix_i^{-1}) \cdot x_iP \\ &= \lambda_i HK_i\end{aligned}$$

– For the verification check, we have that

$$\begin{aligned}g^{\sum_{i=1}^{n} V_i} &= g^{\sum_{i=1}^{n} r_i\psi_{i,0} + \sum_{i=1}^{n} sk_j\psi_{i,1}} \\ &= g^{\sum_{i=1}^{n} r_i\psi_{i,0}} \cdot g^{\sum_{i=1}^{n} sk_j\psi_{i,1}} \\ &= \prod_{i=1}^{n}(g^{r_i})^{\psi_{i,0}} \cdot g^{\sum_{i=1}^{n}(s_j + \gamma H_3(\mathcal{L}_j||T||\Delta_j))\psi_{i,1}} \\ &= \prod_{i=1}^{n} U_i^{\psi_{i,0}} \cdot \prod_{i=1}^{n} \Delta_j^{\psi_{i,1}} \cdot g_0^{\sum_{i=1}^{n} \psi_{i,1} H_3(\mathcal{L}_j||T||\Delta_j)}\end{aligned}$$

The proposed protocol is highly efficient in terms of signature generation and even verification since only 1 point multiplication of $\mathbb{G}_1$, and 2 point multiplications of $\mathbb{G}_1$ and 4 modular exponentiations of $\mathbb{Z}_p^*$ are required in signature generation and verification phases, respectively. Moreover, for n messages with signatures σ_i $(1 \leq i \leq n)$ replied from n vehicles, the receiver aggregately verifies the n signatures to significantly reduce the computational costs.

4 Security Analysis

In this section, we analyze how the proposed protocol satisfies the security objectives stated in Section 2.2.

- **Location Assurance.** This goal can be satisfied by the location-aware credential Σ which is a signature under a location information $\mathcal{L}$ and a time period T. If the location-aware credential in a location-aware signature σ is verified as valid by using the location information $\mathcal{L}$ and the time period T specified in a location-aware message, then the verifier can be convinced that the message was responded by an OBU that passed through the claimed location $\mathcal{L}$ for given time period T because the location-aware credential for the OBU is issued by the RSU physically located in the target geographic area. Moreover, since the location-aware credential is generated by an identity-based aggregate signature scheme [19] which was proven to be secure against adaptive chosen message attacks, no adversary can launch a forgery attack against the location-aware credential.
- **Authentication.** The authenticity of entities that participated in a VANET can be assured by the identity-based secret keys issued through the initial registration in the protocol. That is, only the RSU possessing a valid rk corresponding to its location and the OBU possessing a valid ok derived

from its pseudo identity can be authenticated to each other. Therefore, when we assume the security of the underlying identity-based cryptography, no one can launch an impersonation attack unless the entity is registered to the TA. To forge location-aware signatures based on online/offline signatures [3], and further, an adversary should find collisions of the trapdoor hash value ξ given the corresponding hash key HK. However, this implies the adversary can solve the discrete logarithm problem in $\mathbb{G}_1$, which is computationally infeasible.

- **Location Tracking Avoidance.** In our protocol, message senders and receivers are specified by their hash keys. The distribution of hash key HK is computationally indistinguishable from uniform distribution in $\mathbb{G}_1$ if the probability over the choice of x is uniformly distributed in $\mathbb{Z}_q^*$. Therefore, indistinguishability of hash keys can prevent an adversary from identifying OBUs. In addition, since the hash key is renewed whenever an OBU enters into different geographic areas, an attacker cannot match the originators between observed messages from different locations. As a result, unlinkability of hash keys at different locations can prevent a global eavesdropper from tracking movement of an OBU.
- **Traceability.** In dispute case, the TA is involved in tracing the originator of the message. Given a message formed as shown in Fig. 2, the TA first retrieves the location information $\mathcal{L}_j$ and originator's hash key HK_i from the message. Then the TA requests the pseudo identity PID_i corresponding to the hash key HK_i to the RSU_j located in $\mathcal{L}_j$. On TA's demand, the RSU_j searches the PID_i from its local credential list and responds with the PID_i. Finally, the TA can recover the real identity ID_i by decrypting the PID_i under TA's secret key K.

5 Performance Evaluation

In this section, we evaluate the performance of the proposed protocol in terms of RSU location-aware credential issuance, message processing rate of a responding vehicle, and message processing delay for reply messages. In order to evaluate the processing time of location-aware credential issuance protocol, and location-aware signature generation and verification, we considered PBC library [23] for implementing bilinear pairing and modular operations with 1024 bits security level on Pentium IV 3GHz.

Table 2. The number of cryptographic operations and the processing time

	RSU	OBU	Time(ms)
Credential issuance	$2t_p$+$3t_m$+$1t_e$	$2t_p$+$3t_m$	37.3
Msg. signing	-	$1t_m$	1.9
Msg. verifying	-	$2t_m$+$4t_e$	12.2

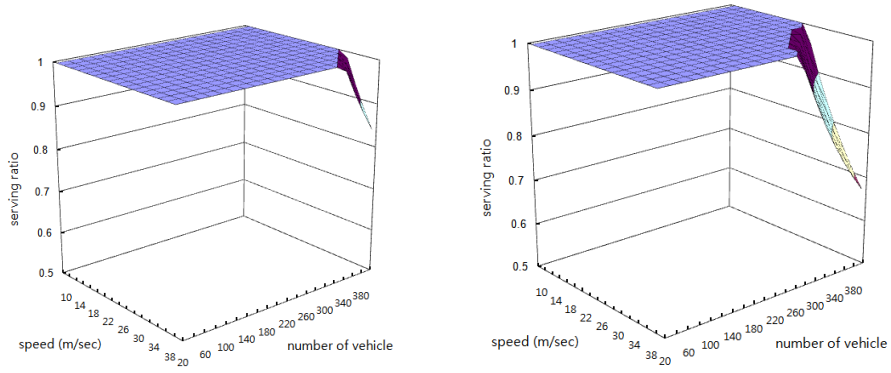
Table 2 shows the measures to estimate the proposed protocol. Since the computations of a bilinear pairing t_p, a point multiplication t_m and a modular exponentiation t_e are much time consuming operations, we did not account any other negligible computation such as cryptographic hash functions.

5.1 Processing of RSU Location-Aware Credential Issuance

The main operation of an RSU is to issue location-aware credentials to vehicles on requests within RSU's valid coverage range R_{rng}. Hence, RSU's performance always depends on vehicles density d and speed v within the coverage range. The RSU valid serving ratio S_{RSU}, which is the fraction of the number of actually issued credentials to the number of requests [13], can be defined by

$$S_{RSU} = \begin{cases} 1, & \text{if} \quad \frac{R_{rng}}{T_k \cdot v} \cdot \frac{1}{d \cdot \rho} \geq 1; \\ \frac{R_{rng}}{T_k \cdot v} \cdot \frac{1}{d \cdot \rho}, & \text{otherwise.} \end{cases}$$

where ρ is the probability for each vehicle to request a location-aware credential and T_k is the execution time of location-aware credential issuance protocol.



(a) valid serving ratio for ρ=0.8 (b) valid serving ratio for ρ=1.0

Fig. 4. RSU valid serving ratio for location-aware credential issuance.

Fig. 4 depicts the RSU valid serving ratio with different vehicle density and different vehicle speed for $R_{rng} = 500$m, and the probability $\rho = 0.8$ and $\rho = 1.0$, respectively. From the results, we can observe that RSU can sufficiently deal with the location-aware credential requests in most practical scenarios even though RSU cannot fully process credential issuance protocol if more than 320 vehicles request their location-aware credentials with the probability greater than 0.8 at the same time. Thus, we conclude that the proposed location-aware credential issuance protocol is feasible.

5.2 Processing of Responding Vehicle

Within a target location area, the valid response processing ratio of a responding vehicle is estimated as the fraction of the actually processed location-aware responses to the number of received requests while the responding vehicle goes through the area after obtaining a location-aware credential. A serving duration T_D for the vehicle passing the target area can be computed as $T_D = (R_{rng}/v) - T_k$. Let T_s and T_v be the processing times for signature generation and verification, respectively. Since the responding vehicle requires a signature verification for a request message and a signature generation for a response message, the number of response N_{res} which the responding vehicle can deal with is measured by $N_{res} = T_D/(T_s + T_v)$. Let N_r be a request message rate per second, and V_n be the average number of requesting vehicle for a target area. Then, the number of request N_{req} received while passing the target area is $N_{req} = (R_{rng}/v) \cdot N_r \cdot V_n$, and then the response ratio S_{res} can be evaluated as N_{res}/N_{req}.

$$S_{res} = \begin{cases} 1, & \text{if } \frac{T_D/(T_s+T_v)}{(R_{rng}/v)\cdot N_r \cdot V_n} \geq 1; \\ \frac{T_D/(T_s+T_v)}{(R_{rng}/v)\cdot N_r \cdot V_n}, & \text{otherwise.} \end{cases}$$

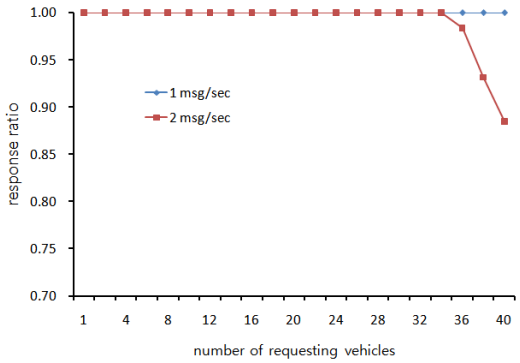


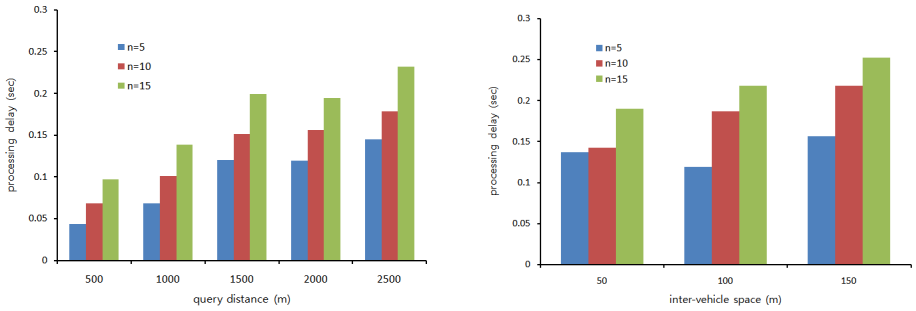
Fig. 5. Serving ratio of a responding vehicle in a target area depending on query message rate.

Fig. 5 depicts serving ratio of a responding vehicle with 20m/s speed in 300m segment area depending on the number of requesting vehicles and message rates. From the results, if a message rate is higher than two messages per second and more than 32 vehicles send request messages, the responding vehicle cannot fully process the all requests. However, location-aware service is an on-demand service and the VITP puts a longer time interval than one second as considering the replying phase processing delay. Consequently, the proposed protocol can practically process almost all location-aware requests in a secure manner.

5.3 Simulation Result

To evaluate the performance for the proposed secure location-aware message query and response over VANETs, we simulated vehicular communications considering highway-traffic scenario by using NS-2 simulator. We used the GPSR [8] as a geographic routing protocol provided by [9] and IEEE 802.11p wireless interface configuration [22] with 11Mbps bandwidth and 250m nominal transmission range.

In our highway-traffic scenario, we deployed vehicles on 5km-long road with 3 lanes to each direction, and fixed target road segment range to 300m. Then, we estimated the message processing delay by varying the query distance to the target area and inter-vehicle space on the road, respectively.



(a) delay to the query distance (b) delay to the inter-vehicle space

Fig. 6. Message processing delay depending on the query distance and the inter-vehicle space with the number of response messages.

The left part in Fig. 6 shows the message processing delays to the query distance from 500m to 2,500m and n response messages within 300m target road segment, where $n = 5, 10, 15$. The delay was measured by end-to-end round-trip time and location-aware signature generation and verification time. However, we did not take into account message loss suffered from routing failure. In addition, the right part in Fig. 6 shows the message processing delays depending on a vehicle density to 2,000m query distance. To measure the processing delay, we varied the inter-vehicle space from 50m to 150m, respectively. From the result, we can observe that the longer inter-vehicle space, which means sparse density, increases the message transmission delay due to much routing processing time.

6 Conclusion

In this paper, we have proposed a novel and efficient privacy-preserving location assurance protocol for providing reliable and trustworthy location-aware

services as well as privacy preservation in VANETs. In particular, we have introduced the notion of location-aware credential based on online/offline signatures and "hash-sign-switch" paradigm to guarantee the trustworthiness of location without violating location privacy. Furthermore, the proposed protocol provides efficient procedures for location-aware signature generation and verification to effectively alleviate computational costs on vehicles in VANETs. We have provided comprehensive analysis to confirm the fulfillment of the security objectives, and the efficiency and effectiveness of the proposed protocol.

References

1. M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," ACM CCS' 93, pp. 62–73, 1993.
2. L. Chen, Z. Chen, and N. P. Smart, "Identity-based key agreement protocols from pairings," International Journal of Information Security, vol. 6, no. 4, pp. 213–241, 2007.
3. X. Chen, F. Zhang, W. Susilo, and Y. Mu, "Efficient generic on-line/off-line sinatures without key exposure," ANCS 2007, LNCS 4521, pp. 18–30, 2007.
4. M. D. Dikaiakos, A. Florides, T. Nadeem, and L. Iftode, "Location-aware services over vehicular ad-hoc networks using car-to-car communication," IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1590–1602, 2007.
5. M. D. Dikaiakos, S. Iqbal, T. Nadeem, and L. Iftode, "VITP: An information transfer protocol for vehicular computing," 2nd ACM Internationial Workshop on Vehicular Ad Hoc Networks (VANET 2005), pp. 30–39, 2005.
6. D. Galindo and F. D. Garcia, "A Schnorr-like lightweight identity-based signature scheme," Africacrypt 2009, LNCS 5580, pp. 135–148, 2009.
7. C. Gentry and Z. Ramzan, "Identity-based aggregate signature," Public Key Cryptography - PKC 2006, LNCS 3958, pp. 257–273, 2006.
8. B. Karp and H. Kung, "Greedy perimeter stateless routing for wireless networks," 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000), pp. 243–254, 2000.
9. W. Kiess, H. Füßler, J. Widmer, and M. Mauve, "Hierarchical location service for mobile ad-hoc networks," ACM Sigmobile Mobile Computing and Communications Review, vol. 8, no. 4, pp. 47–58, 2004.
10. H. Krawczyk and T. Rabin, "Chameleon signatures," Symposium on Network and Distributed Systems Security (NDSS 2000), pp. 143–154, 2000.
11. T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," IEEE Wireless Communications, vol. 13, issue 5, pp. 16–21, 2006.
12. X. Lin, X. Sun, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Transactions on Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, 2007.
13. R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," IEEE INFOCOM 2008, pp. 1229–1237, 2008.
14. T. Nadeem, S. Dashtinezhadd, C. Liao, and L. Iftode, "Trafficview: Traffic data dissemination using car-to-car communication," ACM Sigmobile Mobile Computing and Communications Review, vol. 8, no. 3, pp. 6–19, 2004.

15. Y. Park, C. Sur, C. Jung, and K. H. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications," Journal of Information Science and Engineering, vol. 26, no. 3, pp. 785–800, 2010.
16. V. Pathak, D. Yao, and L. Iftode, "Securing location aware services over VANET using geographical secure path routing," IEEE International Conference on Vehicular Electronics and Safety (ICVES), pp. 346–353, 2008.
17. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.
18. Z. Ren, W. Li, and Q. Yang, "Location verification for VANETs routing," IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 141–146, 2009.
19. S. S. D. Selvi, S. S. Vivek, J. Shriram, and C. P. Rangan, "Efficient and provably secure identity based aggregate signature schemes with partial and full aggregation," Cryptography ePrint Archive, Report 2010/461, 2010.
20. A. Shamir and Y. Tauman, "Improved online/offline signature schemes," Advances in Cryptology - Crypto 2001, LNCS 2139, pp. 355–367, 2001.
21. Dedicated Short Range Communications (DSRC), Available: http://www.leearmstrong.com/dsrc/dsrchomeset.htm.
22. Overhaul of IEEE 802.11 Modeling and Simulation in NS-2, Avaliable: http://dsn.tm.uni-karlsruhe.de/Overhaul_NS-2.php.
23. Pairing-Based Cryptography Library, Available: http://crypto.stanford.edu/pbc.
24. Simulation of Urban Mobility, Available: http://sourceforge.net/projects/sumo.